



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,188	04/24/2001	Ulf Dahl	0104-0334P	2636

26161 7590 10/11/2005
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER

KIM, JUNG W

ART UNIT PAPER NUMBER

2132

DATE MAILED: 10/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

09/840,188

Applicant(s)

DAHL, ULF

Examiner

Jung W. Kim

Art Unit

2132

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 26 September 2005 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires _____ months from the mailing date of the final rejection.
b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
(a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
(b) ☐ They raise the issue of new matter (see NOTE below);
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: _____.
Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____.
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because:

In reply to applicant's argument that there is no motivation to combine the references (Remarks, pg. 4-5), examiner disagrees. Field encryption, the technique of encrypting selected columns of a row of data, was known since 1996. In fact, the Denning reference discloses field encryption techniques, that include:

maintaining records in a table of data in row and column format, at least a portion of the data being encrypted;
maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and
controlling access to the specified proper subset of data in the table according to the separately maintained information.
(see entire Denning document: the disclosure summaries field encryption ["Consider a file of N records where each record has M fields. The objective is to conceal the data in some field of every record. The obvious way of doing this is to encrypt the field under a secret database key K. Letting X_{ij} denote the plaintext value for record i, field j, the ciphertext value $C_{ij}=E_k(X_{ij})$ is thus computed and stored in record i $|i=1...N$ "], pg. 232, last paragraph)] and possible enhancements ["Our solution is simply to use a distinct cryptographic key for each data element; that is, for each record, and for each field within a record. Letting K_{ij} denote the element key for record i, field j, the value X_{ij} is then encrypted as $C_{ij} = E_{K_{ij}}(X_{ij})$ ", pg. 233, section 2.2]).

Further, the reason for encrypting clear values is to ensure that the plaintext values are not retrievable in any context without the proper credentials. Pointedly, the values as stored are encrypted. In the art, there are two notoriously well known reasons for encrypting stored values: first, if a person without the proper decryption keys bypasses security that prevents access to the stored values, the values themselves are still secured from that person, and second, if a person alters encrypted information without knowing the encryption information, the information will be mangled-this preserves integrity of the value. In the Thomson reference, data values are stored in the clear; a security table restricts access by delivering views to a user having proper access credentials. In this case, the clear values still presents a security risk, a risk that would be preventable using the teaching of Denning.

On pg. 2, 2nd paragraph of the Remarks, Applicant argues that the proposed modification is unsatisfactory for its intended purpose, specifically:

"The Examiner proposes to complicate matters considerably by imposing upon Thomson the additional burden of encrypting selected fields and having to somehow manage the keys associated with those fields. As pointed out above, the intended purpose of Thomson is to provide "row security with a minimum amount of effort and time to implement." At the very least, the proposed modification would require some modification to the relation data base software itself, which would now need to distinguish between clear text and encrypted fields, to search for the key that corresponds to an encrypted field, and then to carry out the decryption. This proposed modification is undesirable because it would obviate the expressly-stated advantage of Thompson's solution." (the stated advantage being: "No program changes are required in the relational database software itself, but improved and simplified security is nevertheless available", Remarks, pg. 2, 1st paragraph).

This argument is not persuasive because it is based on the fact that the primary reference discloses the simplicity of the solution is an advantage of Thompson's invention and that the combination with Denning's invention would complicate matters, without offering any additional circumstantial information ("Although statements limiting the function or capability of a prior art device require fair consideration, simplicity of the prior art is rarely a characteristic that weighs against obviousness of a more complicated device with added function." In re Dance, 160 F.3d 1339, 1344, 48 USPQ2d 1635, 1638 (Fed. Cir. 1998) (Court held that claimed catheter for removing obstruction in blood vessels would have been obvious in view of a first reference which taught all of the claimed elements except for a "means for recovering fluid and debris" in combination with a second reference describing a catheter including that means. The court agreed that the first reference, which stressed simplicity of structure and taught emulsification of the debris, did not teach away from the addition of a channel for the recovery of the debris.), MPEP 2143.01).

Regarding Applicant's allegation that a prima facie case of obviousness has not been established (To establish prima facie obviousness, "either the references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references") (Remarks, pgs. 5-6), examiner respectfully disagrees. Case in point, instant claim 18 defines:

A data processing method comprising:

maintaining a database containing a table of data in row and column format, at least a portion of the data being encrypted;
maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and
controlling access to the specified proper subset of data in the table according to the separately maintained information.

Thomson discloses a data processing method comprising:

maintaining a database containing a table of data in row and column format;
maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and
controlling access to the specified proper subset of data in the table according to the separately maintained information.
(see Final Office Action, paragraphs 13 and 14)


Denning discloses a data processing method including:

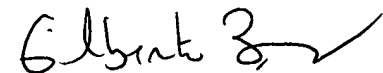
maintaining records in a table of data in row and column format, at least a portion of the data being encrypted;
maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and
controlling access to the specified proper subset of data in the table according to the separately maintained information.
(ibid).

Finally, the reasons for combination are established above and in the action mailed 7/22/05.

In the Remarks, pg. 6-7, Applicant argues that the reference does not inherently store cryptographic information outside the table, specifically Applicant offers a hypothetical example where a data in the column of the table can be encrypted with a user-specific key that is stored with the data in the column ("In fact, it would not be at all unreasonable for Denning to store a key in a table. For example, data in a column of a table can be encrypted with a user-specific key that is stored, after having been encrypted under a common key, with the data in that column", pg. 71st full paragraph). However, Applicant does not provide any basis for the assertion "it would not be at all unreasonable for Denning to store a key in a table". On the contrary, Denning never discloses storing a key value with the data in the same table. All the examples discussed by Denning is under the presumption of concealing data in a given row of a record, not data and key values in a given row ("Consider a file of N records where each record has M fields. The objective is to conceal the data in some field of every record. The obvious way of doing this is to encrypt the field under a secret database key K. Letting X_{ij} denote the plaintext value for record I, field j, the ciphertext value $C_{ij}=E_k(X_{ij})$ is thus computed and stored in record I $|I=1...N$ ", pg. 232, last paragraph). Hence, the Applicant's hypothetical example is not relevant.

Finally, regarding Applicant's argument that Abraham teachings are inconclusive of the missing limitations (Remarks, pgs. 7-8), examiner respectfully disagrees. Denning and Thomson teaches storing information for controlling access to information in a table (ibid). Abraham discloses encrypting data encrypting key values to prevent unscrupulous parties from gaining access to the encrypted data ("The keys used for generation of message authentication codes, encrypting of other keys, and ordinary encryption and decryption tasks can be stored in many places in the secure network. Keys are stored on PC disk memory in encrypted form, encrypted under the master key of one of the security devices. cryptographic adapter 29, card reader 17, or IC card 19. Keys are also stored in the nonvolatile memories of cryptographic adapter 29, card reader 17, and IC card 19.", col. 7:42-50). The Abraham prior art clearly suggests encrypting data encrypting keys anywhere the keys are stored..

 10/5/05


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100